IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND

IN THE MATTER OF THE SEARCH OF **An APPLE iPHONE WITH S/N: 358677233926644**	**Case No.** 23-mj-2189-AAQ

AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR SEARCH WARRANT

I, Brandon Guard, a Postal Inspector with the United States Postal Inspection Service ("USPIS"), being duly sworn, depose and state that:

INTRODUCTION

1. I make this affidavit in support of an application for a search warrant pursuant to the Federal Rule of Criminal Procedure 41 and 18 U.S.C. § 2703(c)(1(A). The property to be search includes one (1) cellular phone, hereinafter referred to as the "**TARGET DEVICE**." Further described in attachment A. This warrant would authorize the examination of property—an electronic device—which is currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B. Specifically, the property to be searched is a blue Apple iPhone, S/N 358677233926644 ("**TARGET DEVICE**")

2. The **TARGET DEVICE** is currently in storage at 900 East Fayette Street, Room 407, Baltimore, MD 21223, which is the USPIS Baltimore Field Office. In my training and experience, and through consultation with other law enforcement officers, I know that the **TARGET DEVICE** has been stored in a manner such that its contents are, to the extent material to this investigation, in substantially the same state as they were when the **TARGET DEVICE** first came into the possession of law enforcement.

3. The applied-for warrant would authorize the forensic examination of the **TARGET DEVICE** for evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 1344 (bank fraud) and 18 U.S.C § 1028A (aggravated identity theft) (collectively the "**TARGET OFFENSES**"). Your affiant believes there is probable cause to search the information described in Attachments A for evidence of these crimes as described in Attachment B

AGENT BACKGROUND

4. I am a Postal Inspector ("Inspector") with the United States Postal Inspection Service ("USPIS") and have been so employed since April 2021. As an Inspector, I investigate offenses that adversely affect the United States Postal Service including robberies, assaults, thefts, contraband mailings, and frauds. Prior to becoming a Postal Inspector, I was employed as a Special Agent with the United States Secret Service ("USSS") from September 2016 to April 2021. In that capacity I conducted complex cyber and financial fraud investigations related to defending the financial infrastructure of the United States. In addition, prior to my federal service, I was employed as a patrol Deputy Sheriff and a State Law Enforcement Agent for 10 years. In those capacities I investigated a variety of crimes including homicide, assault, various frauds, and property crimes. I have received basic and advanced training in the investigation of the above offenses at the Federal Law Enforcement Training Center, The USSS training center, and state law enforcement academies.

5. Based on my experience, training, and knowledge of this investigation and other investigations to date, individuals committing crimes such as identity theft and bank fraud frequently use cellular telephones, communication devices, and other electronic media storage to further their illegal activities. Through my training and experience, and participation in this and other fraud-related investigations, I know that:

a. The fruits, instrumentalities, and evidence of criminal activity are often concealed in digital form. Electronic devices, such as cellular telephones, frequently contain records including video, pictures, location data and private messages related to criminal activity. Furthermore, internet searches are often conducted on cellular telephones in reference to how to commit a crime and news stories related to the crime.

b. Individuals planning fraud activities often use cellular telephones to maintain telephone number "contact lists" of individuals who may have assisted in the planning of this and other criminal activity.

c. Individuals planning fraud activities often use photography and video to document planned location targets, document the criminal activity, and identify areas of egress to be used after the commission of the crimes.

d. Individuals committing fraud activities often use text messages and stored images to coordinate and facilitate the bank fraud activities to include mobile deposits and banking.

e. Finally, based on my training and experience, individuals who commit fraud activities, and other criminal activity, often use cellular telephones to communicate with co-conspirators via phone calls and text messages during preparation, execution, and probable cover up of the fraud activities.

AFFIDAVIT

6. Except where otherwise noted, the information set forth in this affidavit has been compiled personally by me, or provided to me, by other law enforcement officers with whom I have spoken or whose reports I have reviewed. Because this affidavit is submitted for the limited

purpose of seeking the requested search and seizure warrant, I have not set forth each and every fact learned during this investigation.

7. Wherever in this affidavit I discuss information resulting from physical surveillance conducted during this investigation, that information, except where otherwise indicated, does not always set forth my own personal observations, but may have been provided directly or indirectly through other law enforcement officers who conducted such surveillance.

8. Unless otherwise noted, wherever in this affidavit I assert that a statement was made, that statement is described in substance and is not intended to be a verbatim recitation of such statement. Wherever in this affidavit I quote statements, those quotations have been taken from draft transcripts, which are subject to further revision.

9. Unless otherwise stated, the conclusions and beliefs I express in this affidavit are based on my training, experience, and knowledge of the investigation, and reasonable inferences I've drawn from my training, experience, and knowledge of the investigation.

10. Because this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included every known fact to me concerning this investigation. I have set forth only those facts that I believe are sufficient to establish probable cause for the requested warrant. I have not, however, excluded any information known to me that would defeat a determination of probable cause.

JURISDICTION

11. This Court has jurisdiction to issue the proposed warrant because it is a "court of competent jurisdiction" as defined in 18 U.S.C. § 2711. Specifically, the Court is a district court of the United States that has jurisdiction over the offense being investigated, *see* 18 U.S.C. § 2711(3)(A)(i).

PROBABLE CAUSE

12. On July 17, 2023, Baltimore County Police Officers ("BCPD") were dispatched to the M&T Bank located at 2841 Smith Avenue, Mount Washington, MD 21209, on reports of an in-progress fraud incident. Bank staff reported an elderly white female was attempting to withdraw money from an account that did not belong to her. The woman reportedly provided an identification with her photograph but the name on the identification did not match the check. Bank staff reported the woman was dropped off by a black Chevrolet SUV bearing VA registration 755973.

13. Responding BCPD officers encountered and stopped the above referenced Chevrolet SUV. Inside, BCPD Officers identified three male occupants, one of whom was Ali Dickerson ("**Dickerson**")

14. Other responding BCPD officers met with bank staff who explained the female fraud suspect was attempting to negotiate a check (#0102) made out to and endorsed by an apparent identity theft victim with initials "**B.N.**" in the amount of $7,500.00. The suspect claimed to be **B.N.** and was attempting to cash the check written on an account in the same name ending in 4951. While processing the check, bank staff found that M&T Bank's fraud department had placed a fraud alert on the account.

15. Bank staff determined the fraud suspect claiming to be **B.N.** had opened the 4951 account, at the same branch, the week before, at which time she provided a Passport ID card and a Social Security card with **B.N**.'s name. The fraud suspect completed an initial opening check deposit for $50,000.00.

16. The true **B.N.** is the owner of another M&T Bank Business account and is an African American resident of Prince George's County. M&T Bank's fraud department had

contacted the true **B.N.** and confirmed she did not open, or authorize to be opened, any accounts on or about July 10, 2023.

17. BCPD Officers spoke with the fraud suspect, who initially provided officers false information by claiming her name was Brenda Susanne Lewis, but was unable to provide her birthdate. The fraud suspect claimed her husband had dropped her off to deposit the check while he ran errands.

18. As BCPD Officers placed the fraud suspect under arrest, she admitted she had been dropped off by three men in a black vehicle. The fraud suspect said the three men provided her with the checks and fake IDs and sent her into the bank to negotiate the $7500.00 check. The fraud suspect described the men as "a light skinned Black guy [a description matching **Dickerson**'s], a black guy, and the driver is a foreigner." The fraud suspect said she had ridden around with the men to cash checks previously.

19. BCPD Officers spoke with the three men in the black SUV, all of whom denied dropping anyone off at the bank. The men quickly recanted their statements and admitted they dropped a female off at the bank. Officers asked if the female had any property in the vehicle and the men handed officers a stack of paperwork and a dead cell phone. In the papers, Officers found the female's authentic MD identification card and positively identified her as Deborah Suzanne Benaderet (**"Benaderet").** Officers also located a checkbook and partially completed check in the name **B.N.**

20. During transport to the BCPD Pikesville Precinct, **Benaderet** explained that **Dickerson** was the one who provided her with the fake identification documents. **Benaderet** was found to be in possession of controlled substance paraphernalia and the following fraudulent or suspect documents:

a. Fraudulent Passport card, number C97823992, bearing **B.N.'s** name,
b. A copy of an actual Social Security Card, bearing **B.N.'s** name and social security number,
c. Citibank Debit Card, number 4100 3956 3527 3163, bearing **B.N.'s** name**,**
d. M&T Bank Checkbook (for account -4951), checks 103-140, bearing **B.N.'s** name**.**

21. Dickerson was arrested by BCPD and charged for the violation of several fraud related state crimes. The **TARGET DEVICE** was recovered from Dickerson's person by BCPD and was transferred to USPIS.

22. Four weeks earlier, **Dickerson** had pled guilty in the United States District Court for the District of Maryland to theft of mail matter, in violation of 18 U.S.C. § 1708, and admitted to a statement of facts that included his participation in check fraud activities with intended losses of at least $313,000. At the time of this incident, **Dickerson** was on pre-trial release pending sentencing.

23. The incident for which **Dickerson** was charged concerned activities on May 25, 2022, where **Dickerson** and others stole mail from United States Postal Service mail receptacles around Bethesda, Maryland.

24. On that night, Montgomery County, MD, Police ("MCPD") Officers attempted to stop the vehicle in which **Dickerson** was an occupant, a high-speed chase ensued, ending only after multiple MCPD vehicles pinned the suspect vehicle along the roadside to stop it. MCPD Officers found several pieces of non-postmarked mail, personal checks not belonging to any of the occupants, and a USPS "Arrow Key" that provides access to mail receptacles in the area.

25. A warranted search of **Dickerson's** phone, seized upon his arrest on May 25, 2022, yielded evidence he possessed and deposited other stolen checks. Agents believe that **Dickerson's** likely procured the **TARGET DEVICE** at some point afterwards since the earlier-searched phone remains in evidence.

TECHNICAL TERMS

26. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable

storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

c. Portable media player: A portable media player (or "MP3 Player" or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

d. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated "GPS") consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When

a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

e. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments, or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system ("GPS") technology for determining the location of the device.

f. Tablet: A tablet is a mobile computer, typically larger than a phone yet smaller than a notebook, that is primarily operated by touching the screen. Tablets function as wireless communication devices and can be used to access the Internet through cellular networks, 802.11 "wi-fi" networks, or otherwise. Tablets typically contain programs called apps, which, like programs on a personal computer, perform different functions and save data associated with those functions. Apps can, for example, permit accessing the Web, sending and receiving e-mail, and participating in Internet social networks.

g. IP Address: An Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

h. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

27. Based on my training, experience, I know the **TARGET DEVICE** has capabilities that allow it to serve as a wireless telephone, digital camera, portable media player, GPS navigation device, and PDA. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

28. Also, based on my training and experience, I know the **TARGET DEVICE** has the ability to access the internet. Therefore, I submit there is probable cause to search devices for evidence of the various schemes described above, which may constitute violations of the **TARGET OFFENSES**.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

29. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the **TARGET DEVICE**. This information can sometimes be recovered with forensics tools.

30. There is probable cause to believe that things that were once stored on the **TARGET DEVICE** may still be stored there, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few

examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

31. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Device was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the Device because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file

systems can record information about the dates files were created and the sequence in which they were created.

b. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

f. I know that when an individual uses an electronic device to obtain unauthorized access to a victim electronic device over the Internet, the individual's electronic device will generally serve both as an instrumentality for committing the crime,

and also as a storage medium for evidence of the crime. The electronic device is an instrumentality of the crime because it is used as a means of committing the criminal offense. The electronic device is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that an electronic device used to commit a crime of this type may contain data that is evidence of how the electronic device was used; data that was sent or received; and other records that indicate the nature of the offense.

32. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection to determine whether it is evidence described by the warrant.

33. *Manner of execution.* Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

AUTHORIZATION REQUEST

34. Based on the foregoing, I request that the Court issue the proposed search warrant, pursuant to 18 U.S.C. § 2703(c) and Federal Rule of Criminal Procedure 41, based on a finding that there is probable cause to believe **Dickerson**, and others, are engaged in continuing and ongoing fraud related activities. Additionally, I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the **TARGET DEVICE** described in Attachments A to seek the items described in Attachment B.

Respectfully submitted,

Brandon Guard
U.S. Postal Inspector
U.S. Postal Inspection Service

Affidavit submitted by email and attested to me as true and accurate by telephone consistent with Fed. R. Crim. P. 4.1 and 41(d)(3) this 15th day of August 2023.

The Honorable Ajmel A. Quereshi
United States Magistrate Judge

ATTACHMENT A

Property to be Searched

An Apple iPHONE S/N: 358677233926644 (TARGET DEVICE), currently held at the USPIS Baltimore Field Office, located at 900 East Fayette Street Room 407, Baltimore, MD 21233.

ATTACHMENT B

Particular Things to be Seized

1. All records on the **TARGET DEVICE** from May 25, 2022 to present as described in Attachment A that relate to violations of the **TARGET OFFENSES** including:

   a. Any and all communications related to the **TARGET OFFENSES**, including records of incoming and outgoing voice communications; records of incoming and outgoing text messages; records of incoming and outgoing emails; the content of incoming and outgoing text messages and emails; voicemails; voice recordings; contact lists, notes, and associated geographic location data;

   b. Any and all internet browsing history, including internet searches, search terms, and search results, and associated geographic location, related to the **TARGET OFFENSES**;

   c. Records or communications reflecting the receipt of money from the deposit of stolen, altered, or counterfeited checks, credit cards, gift cards, or money orders;

   d. Records or communications created by seeking to steal legitimate identities, creating fake or synthetic identities, including but not limited to images and software used to further identity theft or fraud schemes;

   e. Records or communications relating to the procuring, manufacturing, creating, altering or negotiation of checks, credit cards, United States Treasury checks, gift cards, money orders, and/or identification documents;

   f. Records or communications reflecting the names, addresses and telephone numbers of co-conspirators and telephone toll records for any residential, commercial, and cellular telephone;

g. Records, communications or pictures related to the use of any Postal keys used to steal mail from blue collection boxes or other location;

h. Video, photographs, and any correspondence of activities relating to the theft and/or robbery or Postal keys, theft of mail, use of stolen and/or altered checks, the creation of counterfeit checks using bank account information taken from stolen mail;

i. Any fraudulent activity derived from mail theft generally;

j. All bank records, checks, credit card bills, account information, and other financial records;

k. Any video, photographs, correspondence, or any other files related to obtaining controlled substances by fraud, or the distribution of controlled substances.

2. Evidence of user attribution showing who used or owned the **TARGET DEVICE** at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history.

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

3. If the government identifies any seized communications that may implicate the attorney-client privilege, law enforcement personnel will discontinue its review and take appropriate steps to segregate all potentially privileged information so as to protect it from substantive review. The investigative team will take no further steps regarding any review of information so segregated absent further order of the court. The investigative team may continue

to review any information not segregated as potentially privileged.